National Aeronautics and
Space Administration
Office of the Administrator
Washington, DC 20546-0001

February 1, 2019

TO: Chief Engineer
Associate Administrator for the Science Mission Directorate
Associate Administrator for the Space Technology Mission Directorate
Associate Administrator for the Human Exploration and Operations Mission Directorate

FROM: Associate Administrator

SUBJECT: Direction to Protect Command Link and Other Aspects of Robotic Spacecraft

Identified threats and vulnerabilities to space systems indicate that command uplinks to robotic spacecraft need to be better protected. Consequently, I am directing the protection contained in the enclosure.

I am directing the Chief Engineer to promulgate additional requirements, as appropriate, to implement the intent of this memorandum, and to incorporate these requirements into Agency governance documentation as expeditiously as possible. In case of conflict, Agency governance documentation, once released, will supersede this memorandum.

Stephen G. Jurczyk

Enclosure

cc:
Associate Administrator for Aeronautics Research Mission Directorate
Assistant Administrator for Protective Services

Direction to Protect Command Link and Other Aspects of Robotic Spacecraft

(1) Except for:

a. Spacecraft already required to use command uplink encryption,

b. Hosted instrument payloads,

c. Class C or D spacecraft without a propulsion subsystem, and

d. Spacecraft designed to operate beyond the Moon.

All new-start or newly-solicited robotic spacecraft shall protect the command uplink with encryption compliant with the Federal Information Processing Standard (FIPS) 140-2, Cryptographic Module Validation Program.

> (Rationale: Command link incidents with civil space missions have demonstrated potential impacts to safe operations.)

For robotic spacecraft already in development that would otherwise be subject to this protection, the technical, cost, and schedule impact of adding command link protection shall be analyzed by the Mission Directorate during FY 2019. Command link protection shall be added if it is determined by the Mission Directorate that mission risk is significant and documented in the Project Protection Plan.

The downlink may be encrypted, if determined appropriate by a Mission Directorate, to protect sensitive data.

(2) For all new-start or newly-solicited robotic spacecraft, the command uplink, position, navigation, and timing (PNT) subsystems shall recognize and survive interference.

> (Rationale: Recent GPS incidents with civil space missions showed that missions can unexpectedly lose GPS signals, including timing information.)

(3) For all robotic spacecraft, information pertaining to the command uplink shall be protected at least as Sensitive But Unclassified (SBU), and in accordance with the Asset Vulnerability Protection security classification guide issued by the Office of Protective Services, August 29, 2017.